

# **CIPHERING METHOD, DECIPHERING METHOD, CIPHERING DEVICE, DECIPHERING DEVICE AND RECORDING MEDIUM**

Patent Number: JP2000115551

Publication date: 2000-04-21

Inventor(s): YOKOUCHI KOJI

Applicant(s): FUJI PHOTO FILM CO LTD

Requested Patent: ☐ JP2000115551

Application Number: JP19980278772 19980930

Priority Number(s):

IPC Classification: H04N1/44; G09C1/00; H04L9/06; H04N7/167

EC Classification:

Equivalents:

---

## **Abstract**

---

**PROBLEM TO BE SOLVED:** To reduce the processing time for ciphering compared with the case of ciphering all of image data.

**SOLUTION:** Plural image data is inputted and stored (step 200) and a difference of each image element between one of the plural image data (first image data) and image data excepting for first image data is calculated to be stored as difference data (steps 202 and 204). First image data is ciphered to be stored as ciphered data (step 206) and ciphered data and difference data are retained in a floppy disk as ciphered image data (step 208).

---

Data supplied from the **esp@cenet** database - 12

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-115551/

(P2000-115551A)

(43)公開日 平成12年4月21日(2000.4.21)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テームコード(参考)
H 0 4 N 1/44		H 0 4 N 1/44	5 C 0 6 4
G 0 9 C 1/00	6 1 0	G 0 9 C 1/00	6 1 0 A 5 C 0 7 5
H 0 4 L 9/06		H 0 4 L 9/00	6 1 1 Z 5 J 1 0 4
H 0 4 N 7/167		H 0 4 N 7/167	

審査請求 未請求 請求項の数10 O L (全 12 頁)

(21)出願番号 特願平10-278772

(22)出願日 平成10年9月30日(1998.9.30)

(71)出願人 000005201

富士写真フイルム株式会社

神奈川県南足柄市中沼210番地

(72)発明者 横内 康治

神奈川県足柄上郡開成町宮台798番地 富

士写真フイルム株式会社内

(74)代理人 100079049

弁理士 中島 淳 (外3名)

Fターム(参考) 5C064 CA14 CC04 CC06

5C075 EED3 FF03 FF90

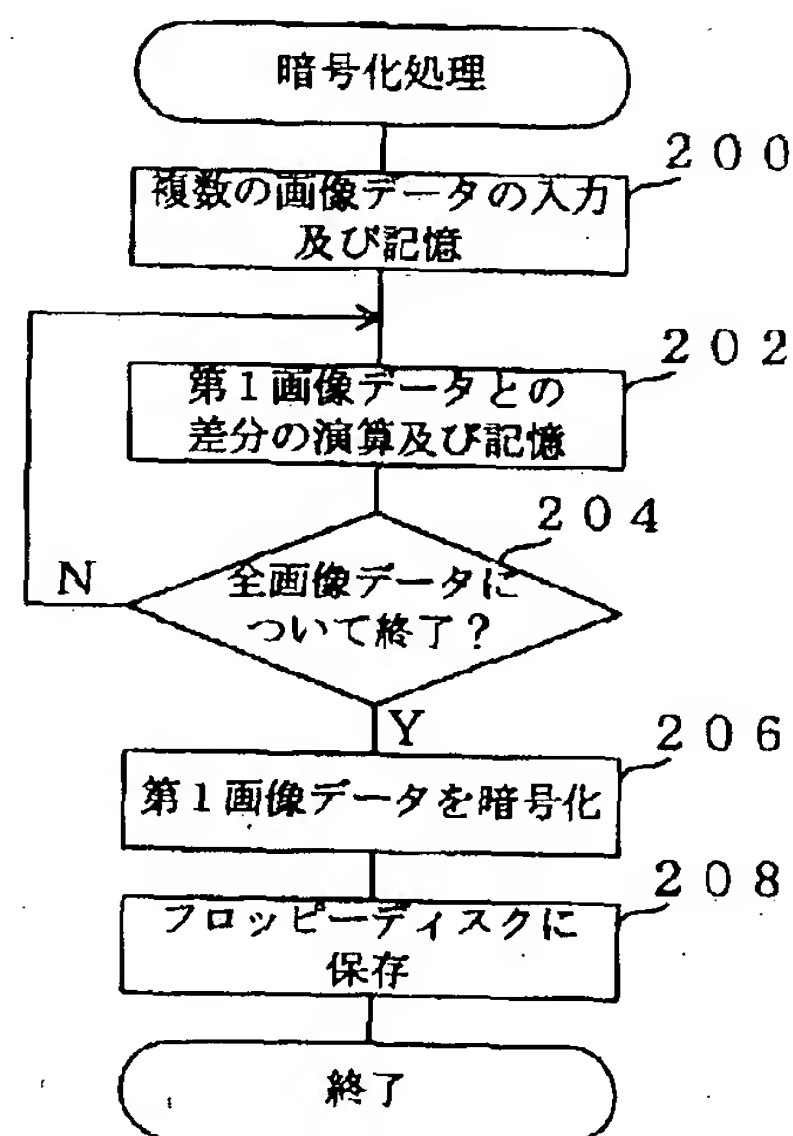
5J104 AA18 CA02 NA02 NA27 PA14

(54)【発明の名称】 暗号化方法、復号化方法、暗号化装置、復号化装置及び記録媒体

(57)【要約】

【課題】 処理時間を短縮することができる暗号化方法、復号化方法、暗号化装置、復号化装置及び記録媒体を得る。

【解決手段】 複数の画像データを入力して記憶し(ステップ200)、該複数の画像データのうちの1つ(第1画像データ)と該第1画像データ以外の画像データとの画素毎の差分を算出して差分データとして記憶し(ステップ202、204)、上記第1画像データを暗号化して暗号化データとして記憶し(ステップ206)、上記暗号化データ及び差分データを暗号化画像データとしてフロッピーディスクに保存する(ステップ208)。



## 【特許請求の範囲】

【請求項1】 各々画像を表す複数の画像データのうちの一部の画像データについては暗号化することにより該一部の画像データに対応する暗号化データを求め、前記複数の画像データのうちの残りの画像データについては前記暗号化する画像データと直接的又は間接的に画素毎の差分を演算することにより前記残りの画像データに対応する差分データを求めることによって前記複数の画像データに対応する暗号化画像データを生成する暗号化方法。

【請求項2】 請求項1記載の暗号化方法によって生成された暗号化画像データを復号化する復号化方法であって、前記暗号化データについては復号化して該暗号化データに対応する画像データを求め、前記差分データについては差分データを求める際に前記暗号化する画像データと直接的に差分を演算した場合は前記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に前記暗号化する画像データと間接的に差分を演算した場合は前記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求めることによって前記暗号化画像データに対応する復号化画像データを生成する復号化方法。

【請求項3】 1画像を表す画像データを複数のブロックに分割し、一部のブロックの画像データについては暗号化することにより該一部のブロックの画像データに対応する暗号化データを求め、前記複数のブロックの画像データのうちの残りのブロックの画像データについては前記暗号化するブロックの画像データと直接的又は間接的に画素毎の差分を演算することにより前記残りのブロックの画像データに対応する差分データを求めることによって前記1画像を表す画像データに対応する暗号化画像データを生成する暗号化方法。

【請求項4】 請求項3記載の暗号化方法によって生成された暗号化画像データを復号化する復号化方法であって、前記暗号化データについては復号化して該暗号化データに対応する画像データを求め、前記差分データについては差分データを求める際に前記暗号化するブロックの画像データと直接的に差分を演算した場合は前記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に前記暗号化するブロックの画像データと間接的に差分を演算した場合は前記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算す

ることにより差分データに対応する画像データを求めることによって前記暗号化画像データに対応する復号化画像データを生成する復号化方法。

【請求項5】 各々画像を表す複数の画像データを入力する画像データ入力手段と、入力された一部の画像データについては暗号化することにより該一部の画像データに対応する暗号化データを求め、入力された残りの画像データについては前記暗号化する画像データと直接的又は間接的に画素毎の差分を演算することにより前記残りの画像データに対応する差分データを求める暗号化手段と、前記暗号化データと前記差分データとを前記複数の画像データに対応する暗号化画像データとして出力する暗号データ出力手段と、を備えた暗号化装置。

【請求項6】 請求項5記載の暗号化装置によって生成された暗号化画像データを復号化する復号化装置であって、前記暗号化データについては復号化して該暗号化データに対応する画像データを求め、前記差分データについては差分データを求める際に前記暗号化する画像データと直接的に差分を演算した場合は前記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に前記暗号化する画像データと間接的に差分を演算した場合は前記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求める復号化手段を備えた復号化装置。

【請求項7】 1画像を表す画像データを入力する画像データ入力手段と、入力された画像データを複数のブロックに分割するブロック化手段と、一部のブロックの画像データについては暗号化することにより該一部のブロックの画像データに対応する暗号化データを求め、前記複数のブロックの画像データのうちの残りのブロックの画像データについては前記暗号化するブロックの画像データと直接的又は間接的に画素毎の差分を演算することにより前記残りのブロックの画像データに対応する差分データを求める暗号化手段と、前記暗号化データと前記差分データとを前記1画像を表す画像データに対応する暗号化画像データとして出力する画像データ出力手段と、を備えた暗号化装置。

【請求項8】 請求項7記載の暗号化装置によって生成された暗号化画像データを復号化する復号化装置であって、前記暗号化データについては復号化して該暗号化データに対応する画像データを求め、前記差分データについては差分データを求める際に前記暗号化するブロックの画



像データと直接的に差分を演算した場合は前記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に前記暗号化するブロックの画像データと間接的に差分を演算した場合は前記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求める復号化手段を備えた復号化装置。

【請求項9】 請求項1乃至請求項4記載のいずれかの発明における処理をコンピュータに実行させるためのプログラムを記録した記録媒体。

【請求項10】 請求項1又は請求項3記載の発明における処理によって生成された暗号化画像データを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、暗号化方法、復号化方法、暗号化装置、復号化装置及び記録媒体に係り、特に、デジタル化された画像データを暗号化する暗号化方法、該暗号化方法を適用可能な暗号化装置、前記暗号化方法をコンピュータで実行させるためのプログラムを記録した記録媒体、前記暗号化方法によって得られた暗号化画像データを記録した記録媒体、前記暗号化方法によって得られた暗号化画像データを復号化する復号化方法、該復号化方法を適用可能な復号化装置、前記復号化方法をコンピュータで実行させるためのプログラムを記録した記録媒体に関する。

【0002】

【従来の技術】従来の画像データに対する暗号化の技術としては、例えば、特開平6-125553号公報に記載の技術があった。

【0003】この特開平6-125553号公報に記載の技術では、暗号化のための処理量を低減することを目的として、画像データに対してDCT変換（離散コサイン変換）を行なうことによって得られた信号のうちの直流成分のみを暗号化していた。

【0004】

【発明が解決しようとする課題】しかしながら、上記特開平6-125553号公報に記載されている技術等の従来の暗号化技術では、暗号化強度を強くするほど、暗号化及び該暗号化によって得られた暗号化画像データの復号化の双方の処理量が多くなるので、暗号化及び復号化のための処理時間が長くなる、という問題点があった。

【0005】また、各々1枚の画像を示す複数の画像データの各々について暗号化及び復号化を行なう場合には、画像データの数に比例して暗号化及び復号化のための処理時間が増加することはいうまでもない。

【0006】本発明は上記問題点を解消するために成さ

れたものであり、処理時間を短縮することができる暗号化方法、復号化方法、暗号化装置、復号化装置及び記録媒体を提供することを目的とする。

【0007】

【課題を解決するための手段】上記目的を達成するために、請求項1記載の暗号化方法は、各々画像を表す複数の画像データのうちの一部の画像データについては暗号化することにより該一部の画像データに対応する暗号化データを求め、前記複数の画像データのうちの残りの画像データについては前記暗号化する画像データと直接的又は間接的に画素毎の差分を演算することにより前記残りの画像データに対応する差分データを求めることによって前記複数の画像データに対応する暗号化画像データを生成する。

【0008】また、請求項5記載の暗号化装置は、各々画像を表す複数の画像データを入力する画像データ入力手段と、入力された一部の画像データについては暗号化することにより該一部の画像データに対応する暗号化データを求め、入力された残りの画像データについては前記暗号化する画像データと直接的又は間接的に画素毎の差分を演算することにより前記残りの画像データに対応する差分データを求める暗号化手段と、前記暗号化データと前記差分データとを前記複数の画像データに対応する暗号化画像データとして出力する暗号データ出力手段と、を備えている。

【0009】請求項1に記載の暗号化方法及び請求項5に記載の暗号化装置によれば、各々画像を表す複数の画像データのうちの一部の画像データについては暗号化することにより該一部の画像データに対応する暗号化データが求められ、上記複数の画像データのうちの残りの画像データについては上記暗号化する画像データと直接的又は間接的に画素毎の差分を演算することにより上記残りの画像データに対応する差分データが求められ、これによって上記複数の画像データに対応する暗号化画像データが生成される。

【0010】ここで、上記暗号化する画像データと間接的に画素毎の差分を演算する場合には、例えば、暗号化データを求める画像データを第1画像データとし、差分データを求める画像データを第N画像データ（ $N=2, 3, \dots$ ）とした場合、第N画像データの差分データを求める際の対象を第（ $N-1$ ）画像データとする場合等が含まれる。但し、この場合、第2画像データの差分データを第1画像データとの差分の演算によって求めることのみは、上記の「直接的」に相当する。

【0011】このように、請求項1に記載の暗号化方法及び請求項5に記載の暗号化装置によれば、複数の画像データの全てを暗号化せずに、一部の画像データのみを暗号化し、残りの画像データについては暗号化する画像データと直接的又は間接的に画素毎の差分を演算することによって全ての暗号化画像データを生成しているの

で、全ての画像データに対して暗号化を行なう場合に比較して暗号化のための処理時間を大幅に短縮することができる。

【0012】また、請求項2記載の復号化方法は、請求項1記載の暗号化方法によって生成された暗号化画像データを復号化する復号化方法であって、前記暗号化データについては復号化して該暗号化データに対応する画像データを求め、前記差分データについては差分データを求める際に前記暗号化する画像データと直接的に差分を演算した場合は前記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に前記暗号化する画像データと間接的に差分を演算した場合は前記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求めることによって前記暗号化画像データに対応する復号化画像データを生成する。

【0013】また、請求項6記載の復号化装置は、請求項5記載の暗号化装置によって生成された暗号化画像データを復号化する復号化装置であって、前記暗号化データについては復号化して該暗号化データに対応する画像データを求め、前記差分データについては差分データを求める際に前記暗号化する画像データと直接的に差分を演算した場合は前記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に前記暗号化する画像データと間接的に差分を演算した場合は前記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求める復号化手段を備えている。

【0014】請求項2に記載の復号化方法及び請求項6に記載の復号化装置は各々、請求項1及び請求項5記載の発明によって生成された暗号化画像データを復号化する復号化方法及び復号化装置であって、上記暗号化データについては復号化して該暗号化データに対応する画像データが求められ、上記差分データについては差分データを求める際に上記暗号化する画像データと直接的に差分を演算した場合は上記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データが求められ、差分データを求める際に上記暗号化する画像データと間接的に差分を演算した場合は上記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データが求められ、これによって上記暗号化画像データに対応する復号化画像データが生成される。

【0015】このように、請求項2に記載の復号化方法及び請求項6に記載の復号化装置によれば、暗号化画像

データの全てを復号化せずに、実際に暗号化された暗号化データのみを復号化し、残りの画像データについては復号化した画像データ又は復号化した画像データに基づく画像データとの加算を行なうことによって全ての復号化画像データを生成しているため、全ての画像データに対して復号化を行なう場合に比較して復号化のための処理時間を大幅に短縮することができる。

【0016】また、請求項3記載の暗号化方法は、1画像を表す画像データを複数のブロックに分割し、一部のブロックの画像データについては暗号化することにより該一部のブロックの画像データに対応する暗号化データを求め、前記複数のブロックの画像データのうちの残りのブロックの画像データについては前記暗号化するブロックの画像データと直接的又は間接的に画素毎の差分を演算することにより前記残りのブロックの画像データに対応する差分データを求めることによって前記1画像を表す画像データに対応する暗号化画像データを生成する。

【0017】また、請求項7記載の暗号化装置は、1画像を表す画像データを入力する画像データ入力手段と、入力された画像データを複数のブロックに分割するブロック化手段と、一部のブロックの画像データについては暗号化することにより該一部のブロックの画像データに対応する暗号化データを求め、前記複数のブロックの画像データのうちの残りのブロックの画像データについては前記暗号化するブロックの画像データと直接的又は間接的に画素毎の差分を演算することにより前記残りのブロックの画像データに対応する差分データを求める暗号化手段と、前記暗号化データと前記差分データとを前記1画像を表す画像データに対応する暗号化画像データとして出力する画像データ出力手段と、を備えている。

【0018】請求項3に記載の暗号化方法及び請求項7に記載の暗号化装置によれば、1画像を表す画像データが複数のブロックに分割され、一部のブロックの画像データについては暗号化することにより該一部のブロックの画像データに対応する暗号化データが求められ、上記複数のブロックの画像データのうちの残りのブロックの画像データについては上記暗号化するブロックの画像データと直接的又は間接的に画素毎の差分を演算することにより上記残りのブロックの画像データに対応する差分データが求められ、これによって上記1画像を表す画像データに対応する暗号化画像データが生成される。

【0019】ここで、上記暗号化するブロックの画像データと間接的に画素毎の差分を演算する場合には、例えば、暗号化データを求めるブロックの画像データを第1画像データとし、差分データを求めるブロックの画像データを第Nブロックの画像データ（ $N=2, 3, \dots$ ）とした場合、第Nブロックの画像データの差分データを求める際の対象を第（ $N-1$ ）ブロックの画像データとする場合等が含まれる。但し、この場合、第2プロ



ックの画像データの差分データを第1ブロックの画像データとの差分の演算によって求めることのみは、上記の「直接的」に相当する。

【0020】このように、請求項3に記載の暗号化方法及び請求項7に記載の暗号化装置によれば、1画像を表す画像データの全ての領域を暗号化せずに、一部のブロックの画像データのみを暗号化し、残りのブロックの画像データについては暗号化するブロックの画像データと直接的又は間接的に画素毎の差分を演算することによって全体的な暗号化画像データを生成しているため、画像データの全ての領域に対して暗号化を行なう場合に比較して暗号化のための処理時間を大幅に短縮することができる。

【0021】また、請求項4に記載の復号化方法は、請求項3に記載の暗号化方法によって生成された暗号化画像データを復号化する復号化方法であって、前記暗号化データについては復号化して該暗号化データに対応する画像データを求め、前記差分データについては差分データを求める際に前記暗号化するブロックの画像データと直接的に差分を演算した場合は前記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に前記暗号化するブロックの画像データと間接的に差分を演算した場合は前記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求めることによって前記暗号化画像データに対応する復号化画像データを生成する。

【0022】また、請求項8に記載の復号化装置は、請求項7に記載の暗号化装置によって生成された暗号化画像データを復号化する復号化装置であって、前記暗号化データについては復号化して該暗号化データに対応する画像データを求め、前記差分データについては差分データを求める際に前記暗号化するブロックの画像データと直接的に差分を演算した場合は前記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に前記暗号化するブロックの画像データと間接的に差分を演算した場合は前記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求める復号化手段を備えている。

【0023】請求項4に記載の復号化方法及び請求項8に記載の復号化装置は各々、請求項3及び請求項7に記載の発明によって生成された暗号化画像データを復号化する復号化方法及び復号化装置であって、上記暗号化データについては復号化して該暗号化データに対応する画像データが求められ、上記差分データについては差分データを求める際に上記暗号化するブロックの画像データと直接的に差分を演算した場合は上記暗号化データに対応

する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に上記暗号化するブロックの画像データと間接的に差分を演算した場合は上記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データが求められ、これによって上記暗号化画像データに対応する復号化画像データが生成される。

【0024】このように、請求項4に記載の復号化方法及び請求項8に記載の復号化装置によれば、暗号化画像データの全ての領域を復号化せずに、一部の領域の画像データに対応する暗号化データのみを復号化し、残りの領域の画像データについては復号化した画像データ又は復号化した画像データに基づいて求めた画像データとの加算を行なうことによって全ての領域の復号化画像データを生成しているため、画像データの全ての領域に対して復号化を行なう場合に比較して復号化のための処理時間を大幅に短縮することができる。

【0025】また、請求項9に記載の記録媒体は、請求項1乃至請求項4に記載のいずれかの発明における処理をコンピュータに実行させるためのプログラムが記録されている。

【0026】従って、コンピュータが前記記録媒体に記録されているプログラムを読み出して実行することにより、請求項1乃至請求項4に記載の発明と同様の効果を奏することができる。

【0027】更に、請求項10に記載の記録媒体は、請求項1又は請求項3に記載の発明における処理によって生成された暗号化画像データが記録されている。

【0028】従って、この記録媒体に記録された暗号化画像データを請求項2及び請求項4に記載の発明によって復号化する場合、復号化に要する処理時間は非常に短い。

【0029】

【発明の実施の形態】以下、図面を参照して、本発明の実施の形態について詳細に説明する。

【0030】〔第1実施形態〕図1に示すように、本第1実施形態に係る暗号化装置及び復号化装置としての暗号化復号化装置10は、パーソナルコンピュータ又はワークステーション等で構成されている。即ち、ディスプレイ32、ワークステーション12、及びワークステーション12に接続された各種の入出力機器を備えている。

【0031】ワークステーション12は、図2に示すように、CPU14、ROM16、RAM18及び入出力ポート20を備え、これらはバスによって互いに接続されている。

【0032】更に、入出力ポート20にはフロッピーディスクに記録された原画像データ、暗号化画像データ等の読み取りやフロッピーディスクへの暗号化画像デー

10

20

30

40

50

タ、復号化画像データ（原画像データ）等の書き込み等に用いられるフロッピーディスクドライブ26が接続されていると共に、暗号化復号化装置10を暗号化装置及び復号化装置として作用させるための暗号化処理プログラム及び復号化処理プログラム等が記憶された記憶装置22が接続されている。暗号化処理プログラム及び復号化処理プログラムは、オペレータからの指示に応じて選択的に読み出されて実行される。

【0033】本第1実施形態では入出力ポート20に接続される入出力機器として、フロッピーディスクドライブ26及び記憶装置22以外に、オペレータが暗号化処理及び復号化処理の何れの処理を行なうのかの指示等を入力するためのキーボード24及びマウス28が用いられている。

【0034】次に、図3を参照して、暗号化復号化装置10を暗号化装置として動作させた場合の暗号化復号化装置10の作用について説明する。なお、図3は、オペレータによって暗号化処理の指示が入力された際に記憶装置22から読み出されて実行される暗号化処理プログラムの概略フローチャートである。

【0035】まずステップ200では、フロッピーディスクドライブ26にセットされているフロッピーディスクに記録されている各々1枚の画像を表す複数の画像データを入力して記憶装置22の所定領域に記憶する。

【0036】次のステップ202では、上記ステップ200において入力及び記憶された複数の画像データのうちの1つの画像データ（以下、第1画像データという。）と該第1画像データ以外の何れかの画像データとの画素毎の差分（以下、差分データという。）を算出して記憶装置22の対応する画像データの記憶領域に記憶（上書き）する。

【0037】次のステップ204では、第1画像データ以外の全ての画像データについて第1画像データとの差分の算出及び記憶が終了したか否かを判定し、終了していない場合は上記ステップ202へ戻り、終了した時点でステップ206に移行する。

【0038】次のステップ206では、上記第1画像データに対して暗号化を行ない、記憶装置22に記憶する。この暗号化の方法としては、公開鍵方式、共通鍵方式等のあらゆる既存の暗号化技術を適用することができる。

【0039】次のステップ208では、上記ステップ206によって記憶装置22に記憶された第1画像データの暗号化データと上記ステップ202及び204の繰り返し処理によって記憶装置22に記憶された第1画像データ以外の画像データの差分データとをフロッピーディスクドライブ26によってフロッピーディスクの空き領域に出力した後、本暗号化処理プログラムを終了する。

【0040】図4には、複数の画像（コマ画像）が記録された1本の写真フィルムの各画像に対応する複数の画

像データを図3に示した暗号化処理プログラムの処理対象とした場合の暗号化画像データ生成の流れが示されている。

【0041】同図に示すように、図3のステップ200の処理によってフロッピーディスクから入力された写真フィルム1本分の複数のコマ画像に各々対応する第1画像データ101、第2画像データ102、第3画像データ103、・・・のうちの第1画像データ101（ステップ206において暗号化される画像データ）以外の画像データは、ステップ202及び204の繰り返し処理によって、第1画像データとの画素毎の差分が算出され、算出された差分データが差分データ102'、差分データ103'、・・・として記憶される。

【0042】その後、ステップ206の処理によって第1画像データ101が暗号化されて暗号化データ101'として記憶される。

【0043】最後にステップ208の処理によって、以上の結果得られた暗号化データ101'、差分データ102'、差分データ103'、・・・が写真フィルム1本分の暗号化画像データとしてフロッピーディスクに保存される。

【0044】次に、図5を参照して、暗号化復号化装置10を復号化装置として動作させた場合の暗号化復号化装置10の作用について説明する。なお、図5は、オペレータによって復号化処理の指示が入力された際に記憶装置22から読み出されて実行される復号化処理プログラムの概略フローチャートである。

【0045】まずステップ250では、フロッピーディスクに記録されている復号化の対象とする暗号化画像データをフロッピーディスクドライブ26によって入力して記憶装置22の所定領域に記憶する。

【0046】次のステップ252では、上記第1画像データに相当する暗号化データに対して復号化を行ない、この結果得られた画像データ、すなわち第1画像データを記憶装置22に記憶する。ここでの復号化方法は暗号化方法に対応した方法とされる。

【0047】次のステップ254では、上記ステップ252によって記憶された第1画像データと、上記ステップ250によって入力及び記憶された暗号化画像データのうちの上記第1画像データ以外の画像データに対応する差分データの1つとの画素毎の和分を算出して記憶装置22の対応する差分データの記憶領域に記憶（上書き）する。本ステップ254によって算出された値は、算出に用いた差分データに対応する画像データに相当する。

【0048】次のステップ256では、全ての差分データについて上記第1画像データとの和分の算出及び記憶が終了したか否かを判定し、終了していない場合は上記ステップ254へ戻り、終了した時点でステップ258に移行する。

10

20

30

40

50



【0049】次のステップ258では、上記ステップ252によって記憶装置22に記憶された第1画像データと上記ステップ254及び256の繰り返し処理によって記憶装置22に記憶された第1画像データ以外の画像データとをフロッピーディスクドライブ26によってフロッピーディスクの空き領域に出力した後、本復号化処理プログラムを終了する。

【0050】図6には、複数の画像（コマ画像）が記録された1本の写真フィルムの各画像に対応する複数の画像データを図3に示した暗号化処理プログラムで暗号化

することによって得られた暗号化画像データを図5に示した復号化処理プログラムの処理対象とした場合の復号化画像データ（原画像データ）生成の流れが示されている。

【0051】同図に示すように、図5のステップ250の処理によってフロッピーディスクから入力された写真フィルム1本分の複数のコマ画像に各々対応する暗号化データ101'、差分データ102'、差分データ103'、・・・のうちの暗号化データ101'は、ステップ252の処理によって復号化されて第1画像データ101として記憶される。

【0052】その後、ステップ254及び256の繰り返し処理によって、第1画像データ101と差分データ102'、103'、・・・との画素毎の和分が算出され、算出された和分が第2画像データ102、第3画像データ103、・・・として記憶される。

【0053】最後にステップ258の処理によって、以上の結果得られた第1画像データ101、第2画像データ102、第3画像データ103、・・・が写真フィルム1本分の復号化画像データ（原画像データ）としてフロッピーディスクに保存される。

【0054】以上詳細に説明したように、本第1実施形態に係る暗号化復号化装置では、暗号化を行なう場合には、暗号化の対象とする複数の画像の画像データの全てを暗号化せずに、1枚の画像に対応する画像データのみを暗号化し、他の画像データについては暗号化する画像データとの差分のみを演算することによって全ての暗号化画像データを生成しているので、全ての画像データに対して暗号化を行なう場合に比較して暗号化のための処理時間を大幅に短縮することができると共に、復号化を行なう場合には、暗号化画像データの全てを復号化せずに、1枚の画像に対応する暗号化データのみを復号化し、他の画像データについては復号化した画像データとの和分のみを演算することによって全ての復号化画像データを生成しているので、全ての画像データに対して復号化を行なう場合に比較して復号化のための処理時間を大幅に短縮することができる。

【0055】なお、本第1実施形態では、第1画像データ以外の画像データの差分を算出する際の対象を第1画像データとした場合について説明したが、本発明はこれ

に限定されるものではなく、例えば、第1画像データ以外の第N画像データ（ $N=2, 3, \dots$ ）の差分を算出する際の対象を第（ $N-1$ ）画像データとすることもできる。このように暗号化画像データを生成した場合、該暗号化画像データを復号する際には暗号化された第1画像データを暗号化方法に対応した復号化方法によって復号した後に、この復号された第1画像データに第2画像データに対応する差分データを画素毎に加算することによって第2画像データを復元し、この第2画像データに対して第3画像データに対応する差分データを画素毎に加算することによって第3画像データを復元する、という手順を第1画像データ以外の全ての画像データについて繰り返すことによって全ての画像データを再現することができる。

【0056】また、本第1実施形態では、実際に暗号化を行なう画像データを1つの画像データのみとした場合について説明したが、本発明はこれに限定されるものではなく、複数の画像データについて暗号化する形態としてもよい。

【0057】また、本第1実施形態では、暗号化処理の途中段階で生成される暗号化データ101'、差分データ102'、・・・や復号化処理の途中段階で生成される第1画像データ101、第2画像データ102、・・・を記憶装置22に記憶する場合について説明したが、本発明はこれに限定されるものではなく、フロッピーディスクに直接記録する形態としてもよい。

【0058】また、本第1実施形態では、差分データを算出する場合の領域を当該画像データの全ての領域とした場合について説明したが、本発明はこれに限定されるものではなく、当該画像データの一部の領域とする形態としてもよい。従って、例えば、第1画像データ101及び第2画像データ102の各々のサイズが異なる場合でも差分データを算出することが可能である。

【0059】また、本第1実施形態では、差分データの各々が、どの画像データとの差分であるのか、といった情報を暗号化画像データに保持しない場合について説明したが、本発明はこれに限定されるものではなく、この情報を保持する形態としてもよい。

【0060】また、本第1実施形態では、暗号化処理プログラム及び復号化処理プログラムを記憶装置22に記録しているが、本発明はこれに限定されるものではなく、該プログラムをフロッピーディスクに記憶すると共に、ワークステーション12にハードディスクを備え、フロッピーディスクから該プログラムを読み取り、ハードディスクにインストールしてもよい。また、有線又は無線のネットワークに電話回線等の伝送手段により伝送してインストールしてもよい。なお、該プログラムをフロッピーディスクに記憶することには限定されず、CD-ROM、磁気テープに該プログラムを格納し、該CD-ROM、磁気テープからパソコンのハードディスクにイ

10

20

30

40

50



インストールしてもよい。また、該プログラムを格納したハードディスクを備えるようにしてもよい。更に、パソコンのハードディスクやRAMに直接プログラムを書き込むようにしてもよい。このように上記プログラムは、有形の記憶媒体及び伝送手段の少なくとも一方により流通することができる。

【0061】また、本第1実施形態では、暗号化画像データをフロッピーディスクに記録する場合について説明したが、本発明はこれに限定されるものではなく、ハードディスク等の磁気ディスク、CD-R等の光ディスク、光磁気ディスク等に記録する形態としてもよい。この場合、上記ハードディスク、CD-R等の各メディアが本発明の請求項10記載の記録媒体に相当することになる。

【0062】〔第2実施形態〕次に、本発明の第2実施形態について説明する。なお、本第2実施形態に係る暗号化装置及び復号化装置としての暗号化復号化装置の構成は、上記第1実施形態（図1及び図2参照）と同様であるので、ここでの説明は省略する。

【0063】まず、図7を参照して、本第2実施形態に係る暗号化復号化装置10を暗号化装置として動作させた場合の暗号化復号化装置10の作用について説明する。なお、図7は、オペレータによって暗号化処理の指示が入力された際に記憶装置22から読み出されて実行される暗号化処理プログラムの概略フローチャートである。

【0064】まずステップ300では、フロッピーディスクドライブ26にセットされているフロッピーディスクに記録されている暗号化の対象とする画像データを入力して記憶装置22の所定領域に記憶する。

【0065】次のステップ302では、上記ステップ300において入力及び記憶された画像データを所定の大きさのブロックに分割する。

【0066】次のステップ304では、上記ステップ302において分割された画像データのうちの1つのブロック（以下、第1ブロックという。）の画像データと該第1ブロック以外のブロックの何れかのブロックの画像データとの画素毎の差分（以下、差分データという。）を算出して記憶装置22の対応するブロックの記憶領域に記憶（上書き）する。

【0067】次のステップ306では、第1ブロック以外の全てのブロックの画像データについて上記第1ブロックの画像データとの画素毎の差分の算出及び記憶が終了したか否かを判定し、終了していない場合は上記ステップ304へ戻り、終了した時点でステップ308に移行する。

【0068】次のステップ308では、上記第1ブロックの画像データに対して暗号化を行ない、記憶装置22に記憶する。この暗号化の方法としては、公開鍵方式、共通鍵方式等のあらゆる既存の暗号化技術を適用するこ

とができる。

【0069】次のステップ310では、上記ステップ308によって記憶装置22に記憶された第1ブロックの画像データの暗号化データと上記ステップ304及び306の繰り返し処理によって記憶装置22に記憶された第1ブロック以外のブロックの画像データの差分データとをフロッピーディスクドライブ26によってフロッピーディスクの空き領域に出力した後、本暗号化処理プログラムを終了する。

10 【0070】図8には、1枚の長尺状の画像に対応する画像データを図7に示した暗号化処理プログラムの処理対象とした場合の暗号化画像データ生成の流れが示されている。

【0071】同図に示すように、図7のステップ300の処理によってフロッピーディスクから入力された画像データ120は、ステップ302の処理によって第1ブロック121、第2ブロック122、第3ブロック123、・・・に分割される。

20 【0072】その後、第1ブロック121、第2ブロック122、第3ブロック123、・・・のうちの第1ブロック121（ステップ308において暗号化されるブロック）以外のブロックの画像データについては、ステップ304及び306の繰り返し処理によって、第1ブロック121の画像データとの画素毎の差分が算出され、算出された差分が差分データ122'、差分データ123'、・・・として記憶される。

【0073】その後、ステップ308の処理によって第1ブロック121の画像データが暗号化されて暗号化データ121'として記憶される。

30 【0074】最後にステップ310の処理によって、以上の結果得られた暗号化データ121'、差分データ122'、差分データ123'、・・・が暗号化画像データとしてフロッピーディスクに保存される。

【0075】次に、図9を参照して、本第2実施形態に係る暗号化復号化装置10を復号化装置として動作させた場合の暗号化復号化装置10の作用について説明する。なお、図9は、オペレータによって復号化処理の指示が入力された際に記憶装置22から読み出されて実行される復号化処理プログラムの概略フローチャートである。

40 【0076】まずステップ350では、フロッピーディスクに記録されている復号化の対象とする暗号化画像データをフロッピーディスクドライブ26によって入力して記憶装置22に記憶する。

【0077】次のステップ352では、上記第1ブロックの画像データに相当する暗号化データに対して復号化を行ない、この結果得られた画像データ、すなわち第1画像データを記憶装置22に記憶する。ここでの復号化方法は暗号化方法に対応した方法とされる。

50 【0078】次のステップ354では、上記ステップ3

52によって記憶された第1画像データと、上記ステップ350によって入力及び記憶された暗号化画像データのうちの第1ブロック以外のブロックの画像データに対応する差分データの1つとの画素毎の和分を算出して記憶装置22の対応する差分データの記憶領域に記憶(上書き)する。本ステップ354によって算出された値は、算出に用いた差分データに対応する画像データに相当する。

【0079】次のステップ356では、第1ブロック以外の全てのブロックの差分データについて上記第1ブロックの画像データとの和分の算出及び記憶が終了したか否かを判定し、終了していない場合は上記ステップ354へ戻り、終了した時点でステップ358に移行する。

【0080】次のステップ358では、上記ステップ352によって記憶装置22に記憶された第1ブロックの画像データと上記ステップ354及び356の繰り返し処理によって記憶装置22に記憶された第1ブロック以外のブロックの画像データとを合成して1つの画像データとした後、次のステップ360では、該1つの画像データをフロッピーディスクドライブ26によってフロッピーディスクの空き領域に出力した後に、本復号化処理プログラムを終了する。

【0081】図10には、1枚の長尺状の画像に対応する画像データを図7に示した暗号化処理プログラムで暗号化することによって得られた暗号化画像データを図9に示した復号化処理プログラムの処理対象とした場合の復号化画像データ(原画像データ)生成の流れが示されている。

【0082】同図に示すように、図9のステップ350の処理によってフロッピーディスクから入力された復号化対象とする暗号化画像データのうちの暗号化データ121'は、ステップ352の処理によって復号化されて第1ブロック121の画像データとして記憶される。

【0083】その後、ステップ354及び356の繰り返し処理によって、第1ブロック121の画像データと差分データ122'、123'、・・・との画素毎の和分が算出され、算出された和分が第2ブロック122の画像データ、第3ブロック123の画像データ、・・・として記憶される。

【0084】最後にステップ358及び360の処理によって、以上の結果得られた第1ブロック121の画像データ、第2ブロック122の画像データ、第3ブロック123の画像データ、・・・が合成されて1枚の画像データに対応する復号化画像データ(原画像データ)120としてフロッピーディスクに保存される。

【0085】以上詳細に説明したように、本第2実施形態に係る暗号化復号化装置では、暗号化を行なう場合には、暗号化の対象とする画像の画像データの全ての領域を暗号化せずに、一部の領域の画像データのみを暗号化し、他の領域の画像データについては暗号化する領域の

画像データとの差分のみを演算することによって全体的な暗号化画像データを生成しているので、画像データの全ての領域に対して暗号化を行なう場合に比較して暗号化のための処理時間を大幅に短縮することができると共に、復号化を行なう場合には、暗号化画像データの全ての領域を復号化せずに、一部の領域の画像データに対応する暗号化データのみを復号化し、他の領域の画像データについては復号化した画像データとの和分のみを演算することによって全ての領域の復号化画像データを生成しているので、画像データの全ての領域に対して復号化を行なう場合に比較して復号化のための処理時間を大幅に短縮することができる。

【0086】なお、本第2実施形態では、第1ブロック以外のブロックの画像データの差分を算出する際の対象を第1ブロックの画像データとした場合について説明したが、本発明はこれに限定されるものではなく、例えば、第1ブロック以外の第Nブロック(N=2、3、・・・)の画像データの差分を算出する際の対象を第(N-1)ブロックの画像データとすることもできる。このように暗号化画像データを生成した場合、該暗号化画像データを復号する際には暗号化された第1ブロックの画像データを暗号化方法に対応した復号化方法によって復号した後に、この復号された第1ブロックの画像データに第2ブロックの画像データに対応する差分データを画素毎に加算することによって第2ブロックの画像データを復元し、この第2ブロックの画像データに対して第3ブロックの画像データに対応する差分データを画素毎に加算することによって第3ブロックの画像データを復元する、という手順を第1ブロック以外の全てのブロックの画像データについて繰り返すことによって全てのブロックの画像データを再現することができる。

【0087】また、本第2実施形態では、実際に暗号化を行なう画像データを1ブロック分の画像データのみとした場合について説明したが、本発明はこれに限定されるものではなく、複数のブロックの画像データについて暗号化する形態としてもよい。

【0088】また、本第2実施形態では、暗号化処理の途中段階で生成される暗号化データ121'、差分データ122'、・・・や復号化処理の途中段階で生成される第1ブロック121の画像データ、第2ブロック122の画像データ、・・・を記憶装置22に記憶する場合について説明したが、本発明はこれに限定されるものではなく、フロッピーディスクに直接記録する形態としてもよい。

【0089】また、本第2実施形態では、差分データを算出する場合の領域を当該ブロックの画像データの全ての領域とした場合について説明したが、本発明はこれに限定されるものではなく、当該ブロックの画像データの一部の領域とする形態としてもよい。従って、例えば、第1ブロック121の画像データ及び第2ブロック12



2の画像データの各々のサイズが異なる場合でも差分データを算出することが可能である。

【0090】また、本第2実施形態では、差分データの各々が、どのブロックの画像データとの差分であるのか、といった情報を暗号化画像データに保持しない場合について説明したが、本発明はこれに限定されるものではなく、この情報を保持する形態としてもよい。

【0091】また、本第2実施形態では、暗号化処理プログラム及び復号化処理プログラムを記憶装置22に記録しているが、本発明はこれに限定されるものではなく、該プログラムをフロッピーディスクに記憶すると共に、ワークステーション12にハードディスクを備え、フロッピーディスクから該プログラムを読み取り、ハードディスクにインストールしてもよい。また、有線又は無線のネットワークに電話回線等の伝送手段により伝送してインストールしてもよい。なお、該プログラムをフロッピーディスクに記憶することに限定されず、CD-ROM、磁気テープに該プログラムを格納し、該CD-ROM、磁気テープからパソコンのハードディスクにインストールしてもよい。また、該プログラムを格納したハードディスクを備えるようにしてもよい。更に、パソコンのハードディスクやRAMに直接プログラムを書き込むようにしてもよい。このように上記プログラムは、有形の記憶媒体及び伝送手段の少なくとも一方により流通することができる。

【0092】また、本第2実施形態では、暗号化画像データをフロッピーディスクに記録する場合について説明したが、本発明はこれに限定されるものではなく、ハードディスク等の磁気ディスク、CD-R等の光ディスク、光磁気ディスク等に記録する形態としてもよい。この場合、上記ハードディスク、CD-R等の各メディアが本発明の請求項10記載の記録媒体に相当することになる。

【0093】

【発明の効果】以上説明したように請求項1及び請求項5記載の発明によれば、複数の画像データの全てを暗号化せずに、一部の画像データのみを暗号化し、残りの画像データについては暗号化する画像データと直接的又は間接的に画素毎の差分を演算することによって全ての暗号化画像データを生成しているため、全ての画像データに対して暗号化を行なう場合に比較して暗号化のための処理時間を大幅に短縮することができる、という効果が得られる。

【0094】また、請求項2及び請求項6記載の発明によれば、暗号化画像データの全てを復号化せずに、実際に暗号化された暗号化データのみを復号化し、残りの画像データについては復号化した画像データ又は復号化した画像データに基づく画像データとの加算を行なうことによって全ての復号化画像データを生成しているため、全ての画像データに対して復号化を行なう場合に比較し

て復号化のための処理時間を大幅に短縮することができる、という効果が得られる。

【0095】また、請求項3及び請求項7記載の発明によれば、1画像を表す画像データの全ての領域を暗号化せずに、一部のブロックの画像データのみを暗号化し、残りのブロックの画像データについては暗号化するブロックの画像データと直接的又は間接的に画素毎の差分を演算することによって全体的な暗号化画像データを生成しているため、画像データの全ての領域に対して暗号化を行なう場合に比較して暗号化のための処理時間を大幅に短縮することができる、という効果が得られる。

【0096】更に、請求項4及び請求項8記載の発明によれば、暗号化画像データの全ての領域を復号化せずに、一部の領域の画像データに対応する暗号化データのみを復号化し、残りの領域の画像データについては復号化した画像データ又は復号化した画像データに基づいて求めた画像データとの加算を行なうことによって全ての領域の復号化画像データを生成しているため、画像データの全ての領域に対して復号化を行なう場合に比較して復号化のための処理時間を大幅に短縮することができる、という効果が得られる。

【図面の簡単な説明】

【図1】実施の形態に係る暗号化復号化装置の外観図である。

【図2】実施の形態に係る暗号化復号化装置の概略構成を示すブロック図である。

【図3】第1実施形態に係る暗号化復号化装置の暗号化処理プログラムの流れを示すフローチャートである。

【図4】第1実施形態に係る暗号化復号化装置の暗号化画像データ生成の流れを示す概念図である。

【図5】第1実施形態に係る暗号化復号化装置の復号化処理プログラムの流れを示すフローチャートである。

【図6】第1実施形態に係る暗号化復号化装置の復号化画像データ（原画像データ）生成の流れを示す概念図である。

【図7】第2実施形態に係る暗号化復号化装置の暗号化処理プログラムの流れを示すフローチャートである。

【図8】第2実施形態に係る暗号化復号化装置の暗号化画像データ生成の流れを示す概念図である。

【図9】第2実施形態に係る暗号化復号化装置の復号化処理プログラムの流れを示すフローチャートである。

【図10】第2実施形態に係る暗号化復号化装置の復号化画像データ（原画像データ）生成の流れを示す概念図である。

【符号の説明】

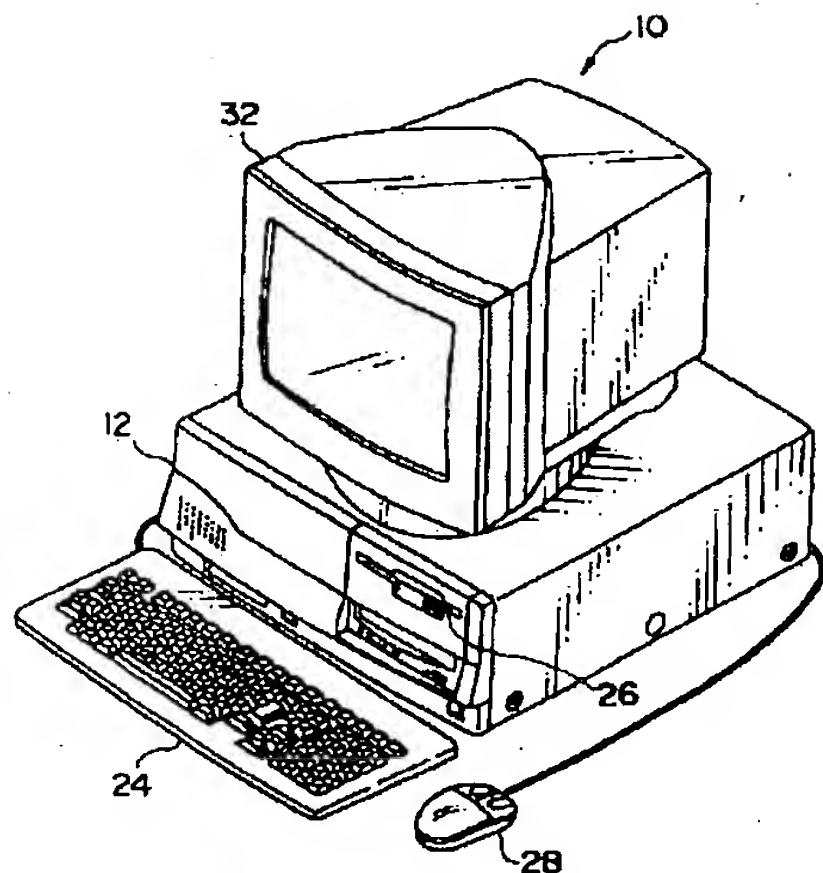
- 10 暗号化復号化装置（暗号化装置、復号化装置）
- 12 ワークステーション／パーソナルコンピュータ
- 14 CPU
- 16 ROM
- 18 RAM



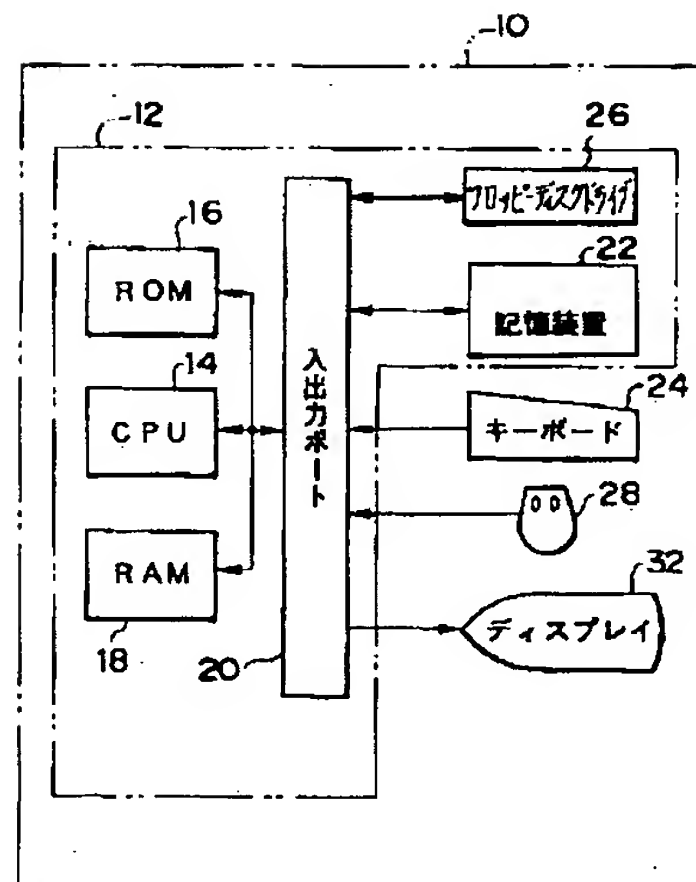
- 20 入出力ポート  
22 記憶装置  
24 キーボード

- 26 フロッピーディスクドライブ  
28 マウス  
32 ディスプレイ

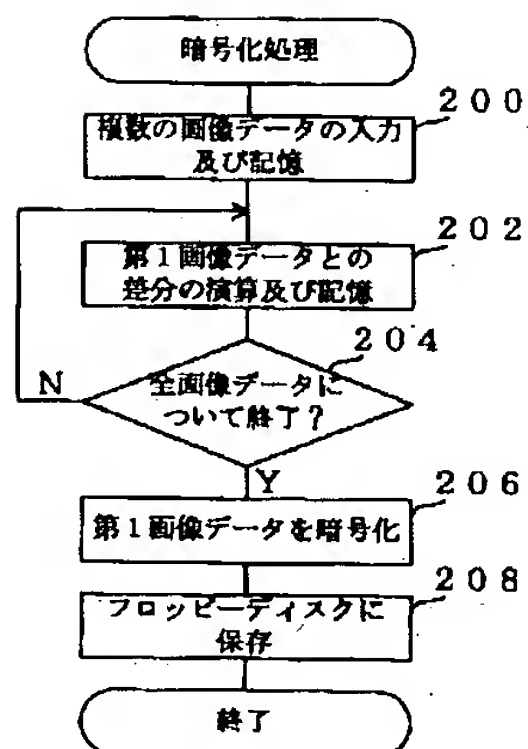
【図1】



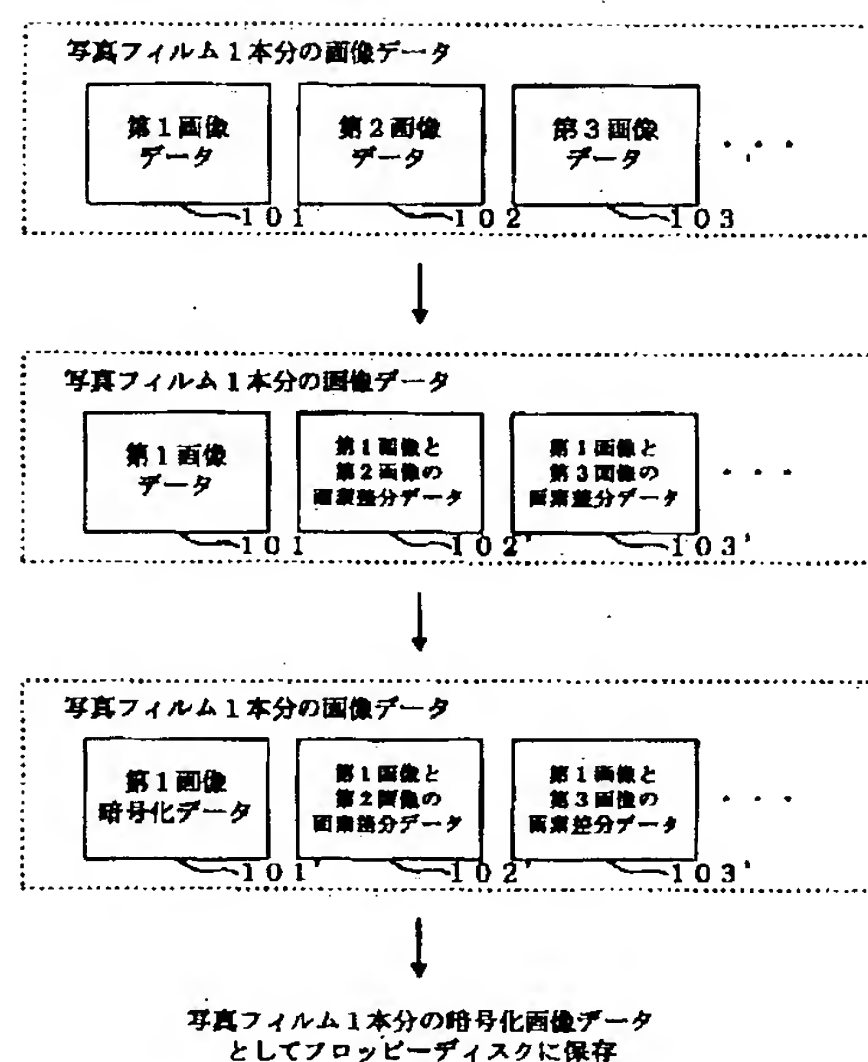
【図2】



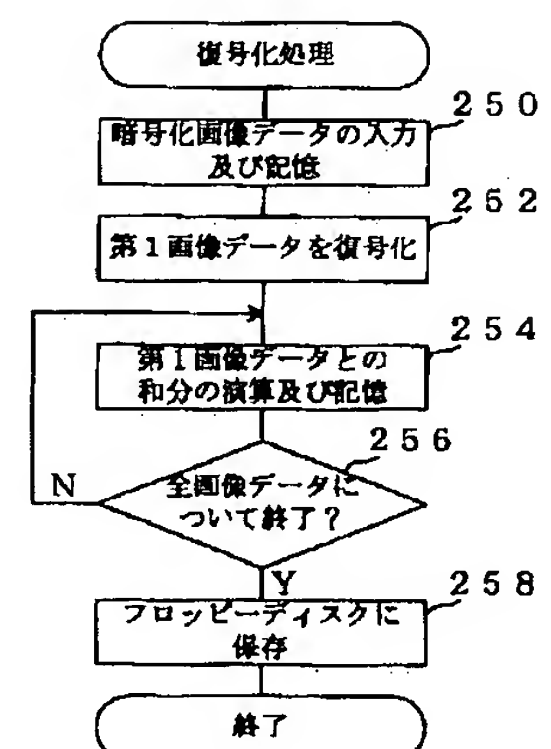
【図3】



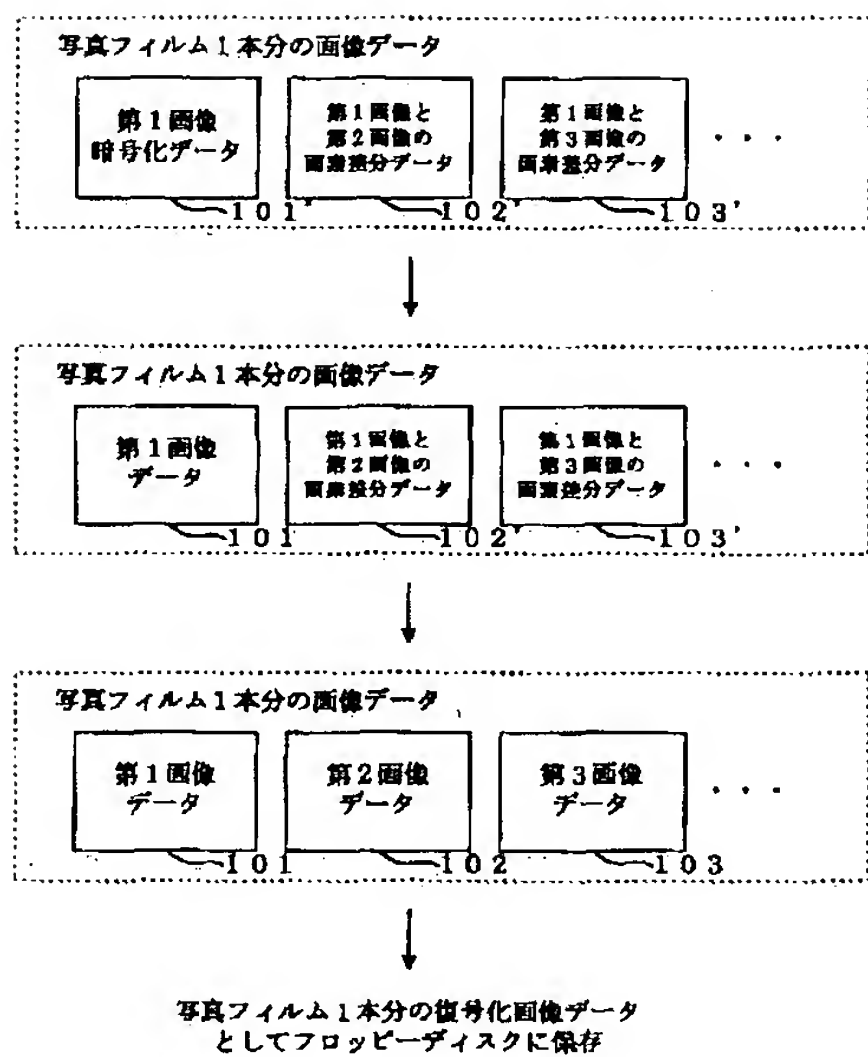
【図4】



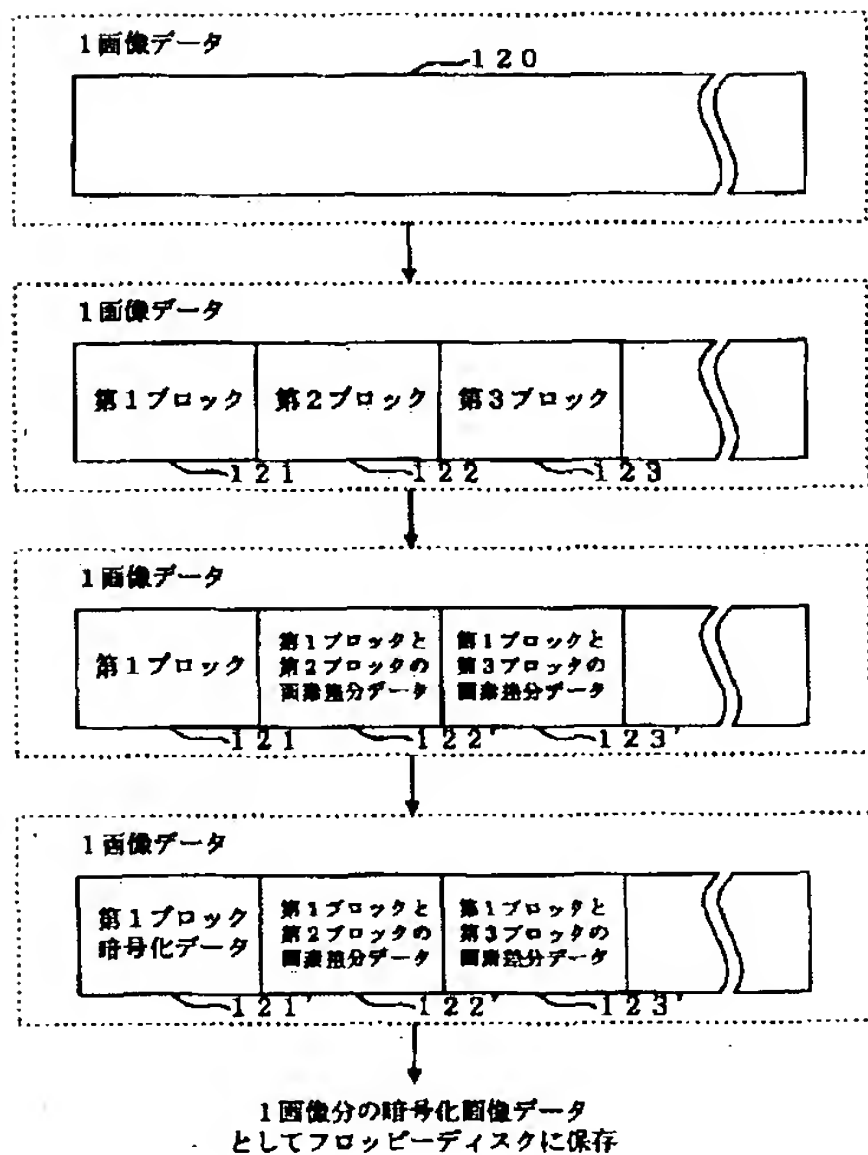
【図5】



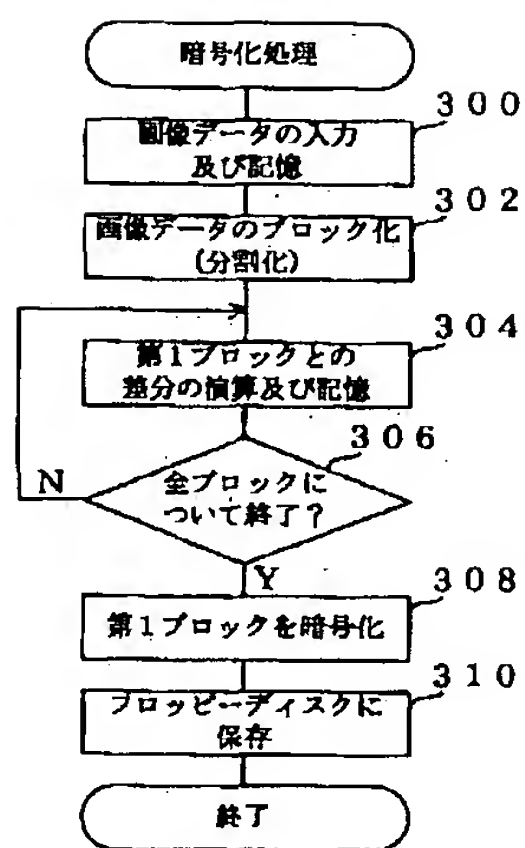
【図6】



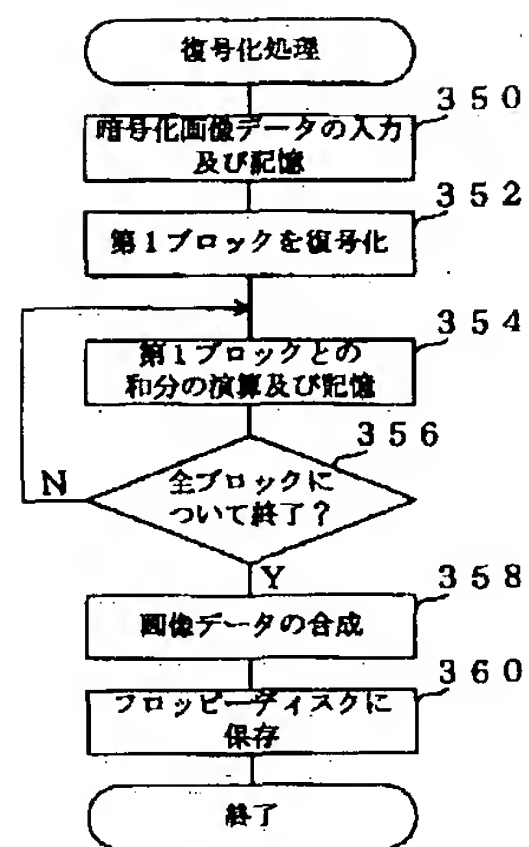
【図8】



【図7】



【図9】



【図10】

